FORM PTO-1390 (Modified) (REV 11-2000) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	
217924US2PCT	
U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	
10/031571	

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/CH99/00336	21 July 1999	none

TITLE OF INVENTION

METHOD AND SUITABLE DEVICES FOR SETTING THE DEGREE OF SECURITY OF CRYPTOGRAPHY FUNCTIONS

APPLICANT(S) FOR DO/EO/US

HUBER Adriano

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include itens (5), (6), (9) and (24) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☒ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).
11. ☐ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☒ A copy of the International Search Report (PCT/ISA/210).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
20. ☐ A second copy of the published international application under 35 U.S.C. 154(d)(4).
21. ☐ A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
22. ☐ Certificate of Mailing by Express Mail
23. ☒ Other items or information:

Form PTO-1449
Drawings (1 sheet)
Amended Sheets (Pages 2, 2a, 8, 9, and 10)

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
10/031571	PCT/CH99/00336	217924US2PCT

24. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☐	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1040.00**	
☒	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$890.00**	
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$740.00**	
☐	International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$710.00**	
☐	International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**	

ENTER APPROPRIATE BASIC FEE AMOUNT =	**$890.00**	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	**$0.00**	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	12 - 20 =	0	x $18.00	**$0.00**	
Independent claims	5 - 3 =	2	x $84.00	**$168.00**	
Multiple Dependent Claims **(check if applicable)**.			☐	**$0.00**	
TOTAL OF ABOVE CALCULATIONS =				**$1,058.00**	
☐ Applicant claims small entity status. See 37 CFR 1.27). The fees indicated above are reduced by 1/2.				**$0.00**	
SUBTOTAL =				**$1,058.00**	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). +				**$0.00**	
TOTAL NATIONAL FEE =				**$1,058.00**	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).** ☐				**$0.00**	
TOTAL FEES ENCLOSED =				**$1,058.00**	
				Amount to be: refunded	$
				charged	$

a. ☒ A check in the amount of **$1,058.00** to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. **15-0030** A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Surinder Sachar
Registration No. 34,423

22850

Surinder Sachar
SIGNATURE

Marvin J. Spivak
NAME

24,913
REGISTRATION NUMBER

Jan 22 2002
DATE

217924US-2 PCT

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF: :

ADRIANO HUBER : ATTN: APPLICATION DIVISION

SERIAL NO: NEW U.S. PCT APPLN :
(BASED ON PCT/CH99/00336)

FILED: HEREWITH :

FOR: METHOD AND SUITABLE DEVICES FOR SETTING THE DEGREE OF SECURITY OF CRYPTOGRAPHY FUNCTIONS

PRELIMINARY AMENDMENT

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

Prior to a first examination on the merits, please amend the above-identified application as follows:

IN THE CLAIMS

Please cancel Claims 1-8 without prejudice.

Please add new Claims 9-20 as follows:

9. (New) A method for setting in a situation-dependent way a degree of security of cryptography functions which are used in at least one communication terminal, which one communication terminal communicates by at least one telecommunication network, in which

method situation-indicating parameters are received in the one communication terminal over the telecommunication network from a secure source, wherein

based on current received situation-indicating parameters, security parameters are determined in the one communication terminal, which security parameters are associated in the one communications terminal with the respective situation-indicating parameters, and which security parameters include at least one of a length of cryptographic keys and a designation of cryptographic algorithms which are used by the cryptography functions and which determine a height of the degree of security of the cryptography functions.

10. (New) The method according to claim 9, wherein at least certain of said situation-indicating parameters contain service-specific data which are transmitted in a secure way over the telecommunication network to the one communication terminal by a service server from which the one communication terminal obtains services.

11. (New) The method according to claim 9, wherein at least certain of said situation-indicating parameters contain data about a permissible degree of security or permissible security parameters which are transmitted in a secure way over the telecommunication network to the one communication terminal by a service server from which the one communication terminal obtains services.

12. (New) The method according claim 9, wherein at least one of said communication terminals is a mobile radio device, and at least one of said situation-indicating parameters contains a country code which is transmitted to the mobile radio device by a mobile radio network in which the mobile radio device is roaming.

13. (New) The method according to claim 10, wherein at least one of said situation-indicating parameters contains data about a permissible degree of security or

permissible security parameters which are transmitted in a secure way over the telecommunication network to the one communication terminal by a service server from which the one communication terminal obtains services.

14. (New) The method according claim 10, wherein at least one of said communication terminals is a mobile radio device, and at least one of said situation-indicating parameters contains a country code which is transmitted to the mobile radio device by a mobile radio network in which the mobile radio device is roaming.

15. (New) The method according claim 11, wherein at least one of said communication terminals is a mobile radio device, and at least one of said situation-indicating parameters contains a country code which is transmitted to the mobile radio device by a mobile radio network in which the mobile radio device is roaming.

16. (New) The method according claim 13, wherein at least one of said communication terminals is a mobile radio device, and at least one of said situation-indicating parameters contains a country code which is transmitted to the mobile radio device by a mobile radio network in which the mobile radio device is roaming.

17. (New) A communication terminal which communicates by a telecommunication network, which communication terminal includes a degree-of-security-determining module in order to set in a situation-dependent way a degree of security of cryptography functions which are used in the communication terminal, which degree-of-security-determining module receives situation-indicating parameters from a secure source in a secure way over the telecommunication network, wherein

the degree-of-security-determining module includes tables or corresponding program instructions by which corresponding security parameters are associated with currently

received situation-indicating parameters, which security parameters include at least one of a length of cryptographic keys and a designation of cryptographic algorithms which are used by the cryptography functions and which determine a height of the degree of security of the cryptography functions.

18. (New) A chipcard which is removably connectible to a communication terminal, which communication terminal communicates by a telecommunication network, which chipcard includes a degree-of-security-determining module in order to set in a situation-dependent way a degree of security of cryptography functions used in the communication terminal, which degree-of-security-determining module receives situation-indicating parameters in a secure way over the telecommunication network from a secure source, wherein

the degree-of-security-determining module includes tables or corresponding program instructions by which corresponding security parameters are associated with currently received situation-indicating parameters, which security parameters include at least one of a length of cryptographic keys and a designation of cryptographic algorithms which are used by the cryptography functions and which determine a height of the degree of security of the cryptography functions.

19. (New) A computer-readable data carrier containing coded data representing a computer program, which computer program is configured to control a processor in a communication terminal, which communication terminal communicates over a telecommunication network, such that the communication terminal sets in a situation-dependent way a degree of security of cryptography functions used in the communication terminal, whereby the communication terminal receives situation-indicating

parameters over the telecommunication network from a secure source in a secure way, wherein

the computer program includes tables or corresponding instructions by which corresponding security parameters are associated with currently received situation-indicating parameters, which security parameters include at least one of a length of cryptographic keys and a designation of cryptographic algorithms which are used by the cryptography functions and which determine a height of the degree of security of the cryptography functions.

20. (New) A computer program element having: computer program code means in order to control a processor in a communication terminal, which communication terminal communicates by a telecommunication network, such that the processor sets in a situation-dependent way a degree of security of cryptography functions used in the communication terminal, whereby the processor receives situation-indicating parameters over the telecommunication network from a secure source in a secure way, wherein

the computer program includes tables or corresponding program instructions by which corresponding security parameters are associated with currently received situation-indicating parameters, which security parameters include at least one of a length of cryptographic keys and a designation of cryptographic algorithms, which are used by the cryptography functions and which determine a height of the degree of security of the cryptography functions.

IN THE ABSTRACT

Please amend the Abstract on page 11 as follows:

ABSTRACT

A method and suitable devices to set the degree of security of cryptography functions in communication terminals in a situation-dependent way. Situation-indicating parameters, for instance a country code for the country in which the communication terminal is momentarily located, are received in a communication terminal, in particular a mobile radio telephone, in a secure way from a secure source by a telecommunication network, in particular a mobile radio network. And, based on received situation-indicating parameters, security parameters are determined in the communication terminal, for instance the maximal permissible bit length of cryptographic keys, which security parameters are used by the cryptography functions and determine the degree of security.

REMARKS

Favorable consideration of this application, as presently amended, is respectfully requested.

The present preliminary amendment is submitted to place the above-identified application in more proper format under United States practice.

By the present preliminary amendment Claims 1-8 are canceled and new Claims 9-20 are presented for examination. New Claims 9-20 are deemed to be self-evident from the original disclosure, including canceled Claims 1-8, and thus are not deemed to raise any issues of new matter. No differences between new Claims 9-20 and canceled Claims 1-8 are believed to narrow the scope of new Claims 9-20.

The Abstract has also been amended to be in more proper format under United States practice.

The present application is believed to be in condition for a full and thorough examination on the merits. An early and favorable consideration of the present application is hereby respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

(703) 413-3000
Fax #: (703)413-2220
SNS/js

I:\atty\SNS\217924US-PR.wpd

Marked-Up Copy
Serial No: _____
Amendment Filed on:
1-22-2002

IN THE CLAIMS

Claims 1-8 (Canceled).

Claims 9-20 (New).

IN THE ABSTRACT

Please amend the Abstract on page 11 as follows:

--A method and suitable devices to set the degree of security of cryptography functions [(11, 23)] in communication terminals [(2)] in a situation-dependent way[, situation-indicating]. Situation-indicating parameters, for instance a country code for the country in which the communication terminal [(2)] is momentarily located, are received in a communication terminal [(2)], in particular a mobile radio telephone [(2)], in a [secured] secure way from a secure source [(3, 4) via] by a telecommunication network [(3)], in particular a mobile radio network [(3), and]. And, based on received situation-indicating parameters, security parameters are determined in the communication terminal [(2)], for instance the maximal permissible [(bit)] bit length of cryptographic keys, which security parameters are used by the cryptography functions [(11, 23)] and determine the degree of security.

[(sole figure)]--

1/prts

Method and Suitable Devices for Setting the Degree of Security of Cryptography Functions

This invention relates to a method and suitable devices for setting the degree of security of cryptography functions. In particular, this invention relates to a method and suitable devices for setting the degree of security of cryptography functions used in communication terminals.

It is common practice today to use cryptography methods to protect confidential data from being accessed by unauthorized third parties during transmission over telecommunication networks, in particular during transmission over mobile radio networks, by means of which cryptography methods the confidential data are encrypted by the sender before being transmitted over the telecommunication network and are decrypted by the recipient after being transmitted over the telecommunication network. Different cryptography methods have different degrees of security, depending upon security parameters such as the cryptography algorithms used and the cryptographic keys applied therein, in particular the bit length of the keys used therein. The users of the cryptography methods, for example service providers, such as financial institutions, or those availing of services, such as bank clients, generally desire a high degree of security. However, national interests of certain countries in which, for example, respective cryptographic products are produced and/or in which holders of respective protective rights reside, call for preventing the dissemination of cryptography products, for example starting at certain predefined degrees of security or using certain predefined security parameters, beyond national borders or at least into certain predefined countries. For the producers of such cryptography products, who, in their own economic interests, would like to market their products worldwide as much as possible, but who are subject to national regulations and legal stipulations, the problem then arises of how they can pursue their own interests as efficiently as possible while respecting national regulations. Producing, administering and maintaining different cryptography products for different markets has not proven to be an optimal solution since the product versions and in particular also combinations with other products, in which cryptography products are integrated, are far too numerous and entail an uneconomical additional expense. In alternative solutions, the same product is supplied everywhere, but certain parts subject to the imposed national restriction regulations are

deactivated by switches before product delivery, for instance by means of software switches switched on or off by setting so-called flags. The problem with this alternative solution is that these switches can often be changed also by third parties, for example through so-called program patches that are able to manipulate the mentioned flags.

Described in the patent application EP 779 760 A1 is a method to indicate to a respective user in a mobile station whether the data transmission between the mobile station and the mobile communications system is encrypted or not. To achieve this, according to the teachings of EP 779 760 A1, the signals exchanged between the mobile station and the mobile communications system are monitored, and on the basis of the monitored signals it is indicated to the user whether the exchanged data are encrypted or not, for example by reproducing different acoustical signals for the user for the encrypted mode and for the unencrypted mode. In accordance with GSM standards (Global System for Mobile Communication), the encryption mode according to EP 779 760 A1 is set in the encrypted mode, or respectively in the unencrypted mode, by units in the mobile communications system by means of so-called "cipher code command" messages. According to the teaching of EP 779 760 A1, the current encryption mode can be indicated by the central processor of the mobile station, for example, in a display data field provided therefor which comprises e.g. a single information bit.

It is an object of this invention to propose a new and better method as well as devices suitable therefor which make it possible to set the degree of security of cryptography functions used in communication terminals, in particular in a situation-dependent way.

This object is achieved according to the present invention through the elements of the independent claims. Further advantageous embodiments follow moreover from the dependent claims and from the specification.

This object is achieved through the present invention in particular in that situation-indicating parameters from a secure source, which is authenticated as a secure source by means of a digital certificate, for example, are received via the telecommunication network in a secure way, e.g. directly, without

possibilities of being influenced by other elements, in a communication terminal that communicates over telecommunication networks from an encoded data object with certified key or as a component, which cannot be influenced, of the protocol used in the respective telecommunication network, and in that security parameters, for instance the maximal permissible length of cryptographic keys or permitted cryptographic algorithms, are determined in the communication terminal based on received situation-indicating parameters. These security parameters are then used by cryptography functions and determine the degree of security. The advantage of this method is that the degree of security of cryptography functions used in the communication terminal, or respectively of the security parameters applied by these cryptography functions, can be set situation-dependently and dynamically so that differing cryptography products do not have to be supplied in different destination markets and no switches have to be set by manufacturers in a fixed way, the effect of which switches can be cancelled by one-time overwriting.

In an embodiment variant, at least certain situation-dependent parameters contain service-specific data, for example data relating to the type of respective service, which are transmitted in a secure way, e.g. encrypted

and/or as a component of a digital, encoded data object with certified key, over the telecommunication network to the communication terminal by a service server, for instance an e-mail server or a file-transfer server from which the said communication terminal obtains services. The advantage of taking into account service-specific data in determining the degree of security of cryptography functions is that different degrees of security can be prescribed and set for different services, e.g. higher degrees of security for financial services than for e-mail services, for different levels of services, e.g. differing degrees of security on the transport level and on the application level, and for different applications of services, e.g. different degrees of security for file transfer in a financial application (financial service) than in a database application (data service).

In an embodiment variant, at least certain situation-indicating parameters contain data about the permissible degree of security, for instance according to an internationally agreed-upon standard or permissible security parameters, e.g. data about specific permissible cryptographic algorithms, which are transmitted to the communication terminal over the telecommunication network in a secure way, for example encrypted and/or as a component of a digital, encoded data object with certified key, by a service server from which the communication terminal obtains services.

In an embodiment variant, at least certain of the communication terminals are mobile radio devices, for example mobile radio telephones or communication-capable laptop or palmtop computers for GSM (Global System for Mobile Communication), UMTS (Universal Mobile Telephone System) or other, for instance satellite-based, mobile radio networks, and at least certain situation-indicating parameters contain a country code which is transmitted to the mobile radio device by a mobile radio network in which the mobile radio device is roaming. Application of the method according to the invention in mobile radio devices, in particular using country codes as situation-indicating parameters, has the advantage that the degree of security of the cryptography functions used can be dynamically adapted to the restrictions concerning permissible maximal degrees of security valid in a respective country of location.

It should be mentioned here that, besides a method according to the invention, the present invention also relates to a communication terminal according to the invention, in particular to a mobile communication terminal, for example a mobile radio telephone or a communication-capable laptop or palmtop computer for GSM, UMTS or other, e.g. satellite-based, mobile radio networks, to a chipcard according to the invention, for example an SIM card (Subscriber Identification Module), which can be inserted into a communication terminal, as well as to a computer-readable data carrier according to the invention and to a computer program element according to the invention.

An embodiment of the present invention will be described in the following with reference to an example. The example of the embodiment will be illustrated by the following sole attached figure:

Figure 1 shows a block diagram with a schematic illustration of a first mobile radio device with a chipcard, a second mobile radio device as well as a service server which are connected to a mobile radio network.

The reference numeral 3 in Figure 1 refers to a telecommunication network, in particular a mobile radio network 3, e.g. a GSM, UMTS or other, e.g. satellite-based, mobile radio network 3, via which network communication terminals 2, in particular mobile radio devices 2, are able to communicate, i.e. in particular exchange data, with one another or with service servers 4, for example a file transfer server, a finance server, a database server, or an e-mail server.

The mobile radio devices 2 include a degree-of-security-determining module 12, 24 according to the invention, which is preferably a programmed software module located in a suitable data store, that cannot be manipulated by users, in the mobile radio device 2 or on a chipcard 1 connected to the mobile radio device 2. The degree-of-security-determining module 12, 24, is, for example, a component of cryptography functions 11, 23 which are used in the mobile radio devices 12, 24. Functions of the degree-of-security-determining module 12, 24 are executed in a processor in the mobile radio device 2 or on the chipcard 1 connected to the mobile radio device 2.

The main function of the degree-of-security-determining module 12, 24 is to set in a situation-dependent way the degree of security of the cryptography functions 11, 23 used in the mobile radio device 2, or respectively of the

security parameters used by these cryptography functions 11, 23. The current situation is thereby determined by so-called situation-indicating parameters which are received by the degree-of-security-determining module 12, 24 from secure sources.

Considered as situation-indicating parameters are the respective country in which the mobile radio device 2 is being operated or service-specific data, for instance the respective service or type of service of a service server 4 being used by the mobile radio device 2, or data relating to protocols or protocol levels, which are used by this service, or other data about the respective service, or data about how a particular service or an available function is used. For instance, for the use of file-transfer functions in a finance application (financial service), a higher degree of security can be permissible than for their use in a database application (data service). It is also possible for the situation-indicating parameters to contain direct and specific data relating to the security parameters to be used, or relating to the degree of security to be used and/or to the maximal permissible degree of security. Data relating to the degree of security are preferably based on an international standard.

Considered security parameters are, for example, the (bit) length of cryptographic keys used or the designation of specific cryptographic algorithms to be used from a series of possible alternative algorithms.

A source of situation-indicating parameters, for example the service server 4, can then be accepted as secure if, for instance, a digital (signed) certificate is received from it authenticating the source. The network infrastructure of the mobile radio network 3 can be considered as a secure source in the sense that components, which cannot be influenced, of the protocol used in the mobile radio network are used as situation-indicating parameters.

Situation-indicating parameters are received securely over the telecommunication network in the sense that they are received directly, without possibilities of being influenced by other elements, e.g. from a digital, encoded data object with certified key or as a component that cannot be influenced from the protocol data units of the protocol used in the respective mobile radio network 3.

For conversion of received situation-indicating parameters into security parameters to be used, the degree-of-security-determining module 12, 24 has at its disposal, for example, corresponding tables, which cannot be manipulated by the user, or corresponding program instructions, by means of which corresponding security parameters are associated with the current, received situation-indicating parameters. Since the permissible degree of security, or respectively the security parameters, can change in the course of time, in particular in different countries, it is possible to update these tables, or respectively these program instructions, with the aid of secure cryptographic functions in a responsible service center or via the mobile radio network 3.

Situation-indicating parameters are captured by the degree-of-security-determining module 12, 24 in that, for instance, protocol data units received over the mobile radio network 3 are checked as to whether they contain a new country code (MCC, Mobile Country Code), or in that encoded data objects with certified key (digital certificates) received over the mobile radio network 3 are checked as to whether they contain situation-indicating parameters, for instance service-specific data such as, for example, an indication concerning the current type of service, e.g. e-mail or file-transfer, or concerning the use of a service, e.g. the use of file-transfer in a finance application (financial service) or in a database application (data service). One skilled in the art will understand that it is also possible to define special protocols for determining situation-indicating parameters, or respectively for determining degrees of security and/or the security parameters to be applied, which special protocols can be used between communication terminals 2, in particular the degree-of-security-determining module 12, 24 contained therein, and service servers 4.

It should also be mentioned here that situation-indicating parameters and the differentiation of the degrees of security to be applied, or respectively the security parameters, can also relate to individual protocol levels, for example protocol levels according to the seven-layered OSI reference model (Open Systems Interconnection) of the ISO (International Standards Organization), so that, for instance, for the applications level (OSI level 7) and the transportation level (OSI level 4), different restrictions regarding permissible degrees of security are applicable. It should also be mentioned here that typically a plurality of situation-indicating parameters are combined, so that, for example, in the country "X" and in the country "Y" the same

restrictions can apply on the transport level, but stricter restrictions apply on the application level for country "X" than for country "Y."

Changes in the degree of security of the cryptography functions 11, 23 used in the mobile radio device 2, or respectively in the security parameters used by these cryptography functions 11, 23 can be reported to the user by means of the display 21, for instance through programmed functions of the degree-of-security-determining module 12, 24. It is also possible for the user of the mobile radio device 2 to be able to inform himself about the current degrees of security or the momentarily used security parameters by activating, for instance, correspondingly programmed functions of the degree-of-security-determining module 12, 24, e.g. by means of the operating elements 22 of the mobile radio device 2.

Besides the initially mentioned advantages for the producers of products with cryptographic functions (11, 23), there are also possibilities for direct commercial marketing of the present invention. For example, communication terminals and/or chipcards can be manufactured and sold which include a degree-of-security-determining module according to the invention. It is also possible to produce and to sell, or provide under licensing fees, computer-readable data carriers containing coded data representing a computer program that makes it possible to control a processor, in particular in a communication terminal, in such a way that it sets the degree of security of cryptography functions (11, 23) used, or respectively of security parameters applied by these cryptography functions (11, 23), in a situation-dependent way according to the method described. Computer program elements including computer program code means for controlling a processor, in particular a processor in a communication terminal, in such a way that it sets the degree of security of cryptography functions (11, 23) used, or of security parameters applied by these cryptography functions (1, 23), in a situation-dependent way according to the method described, can be provided to third parties in exchange for payment of licensing fees, which third parties can integrate these computer program elements into the most various devices.

Claims

1. A method for setting in a situation-dependent way the degree of security of cryptography functions (11, 23) which are used in communication terminals (2), which communication terminals (2) communicate via telecommunication networks (3), in which method situation-indicating parameters are received in a said communication terminal (2) over the telecommunication network (3) from a secure source (3, 4), wherein

based on current received situation-indicating parameters, security parameters are determined in the said communication terminal (2), which security parameters are associated in the communications terminal (2) with the respective situation-indicating parameters, and which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).

2. The method according to claim 1, wherein at least certain said situation-indicating parameters contain service-specific data which are transmitted in a secure way over the telecommunication network (3) to the said communication terminal (2) by a service server (4) from which the said communication terminal (2) obtains services.

3. The method according to one of the claims 1 or 2, wherein at least certain said situation-indicating parameters contain data about the permissible degree of security or permissible security parameters which are transmitted in a secure way over the telecommunication network (3) to the said communication terminal (2) by a service server (4) from which the said communication terminal (2) obtains services.

4. The method according to one of the claims 1 to 3, wherein at least certain said communication terminals (2) are mobile radio devices, and at least certain said situation-indicating parameters contain a country code which is transmitted to the said mobile radio device (2) by a mobile radio network (3) in which the said mobile radio device (2) is roaming.

5. A communication terminal (2) which communicates via a telecommuni-

cation network (3), which communication terminal (2) includes a degree-of-security-determining module (12, 24) in order to set in a situation-dependent way the degree of security of cryptography functions (11, 23) which are used in the communication terminal (2), which degree-of-security-determining module (12, 24) receives situation-indicating parameters from a secure source (3, 4) in a secure way over the telecommunication network (3), wherein

the degree-of-security-determining module (12, 24) includes tables or corresponding program instructions by means of which corresponding security parameters are associated with the current received situation-indicating parameters, which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).

6. A chipcard (1) which is removably connectible to the communication terminal (2), which communication terminal (2) communicates via a telecommunication network (3), which chipcard (1) includes a degree-of-security-determining module (12) in order to set in a situation-dependent way the degree of security of cryptography functions (11) used in the communication terminal (2), which degree-of-security-determining module (12) receives situation-indicating parameters in a secure way over the telecommunication network (3) from a secure source (3, 4), wherein

the degree-of-security-determining module (12) includes tables or corresponding program instructions by means of which corresponding security parameters are associated with the current received situation-indicating parameters, which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).

7. A computer-readable data carrier containing coded data representing a computer program, which computer program makes it possible to control a processor in a communication terminal (2), which communication terminal (2) communicates over a telecommunication network (3), such that it sets in a situation-dependent way the degree of security of cryptography functions (11,

23) used in the communication terminal (2), whereby it receives situation-indicating parameters over the telecommunication network (3) from a secure source (3, 4) in a secure way, wherein

the computer program includes tables or corresponding instructions by means of which corresponding security parameters are associated with the current received situation-indicating parameters, which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).

8. A computer program element having: computer program code means in order to control a processor in a communication terminal (2), which communication terminal (2) communicates via a telecommunication network (3), such that the processor sets in a situation-dependent way the degree of security of cryptography functions (11, 23) used in the communication terminal (2), whereby it receives situation-indicating parameters over the telecommunication network (3) from a secure source (3, 4) in a secure way, wherein

the computer program includes tables or corresponding program instructions by means of which corresponding security parameters are associated with the current received situation-indicating parameters, which security parameters include the length of cryptographic keys and/or the designation of cryptographic algorithms, which are used by the said cryptography functions (11, 23) and which determine the height of the degree of security of these said cryptography functions (11, 23).

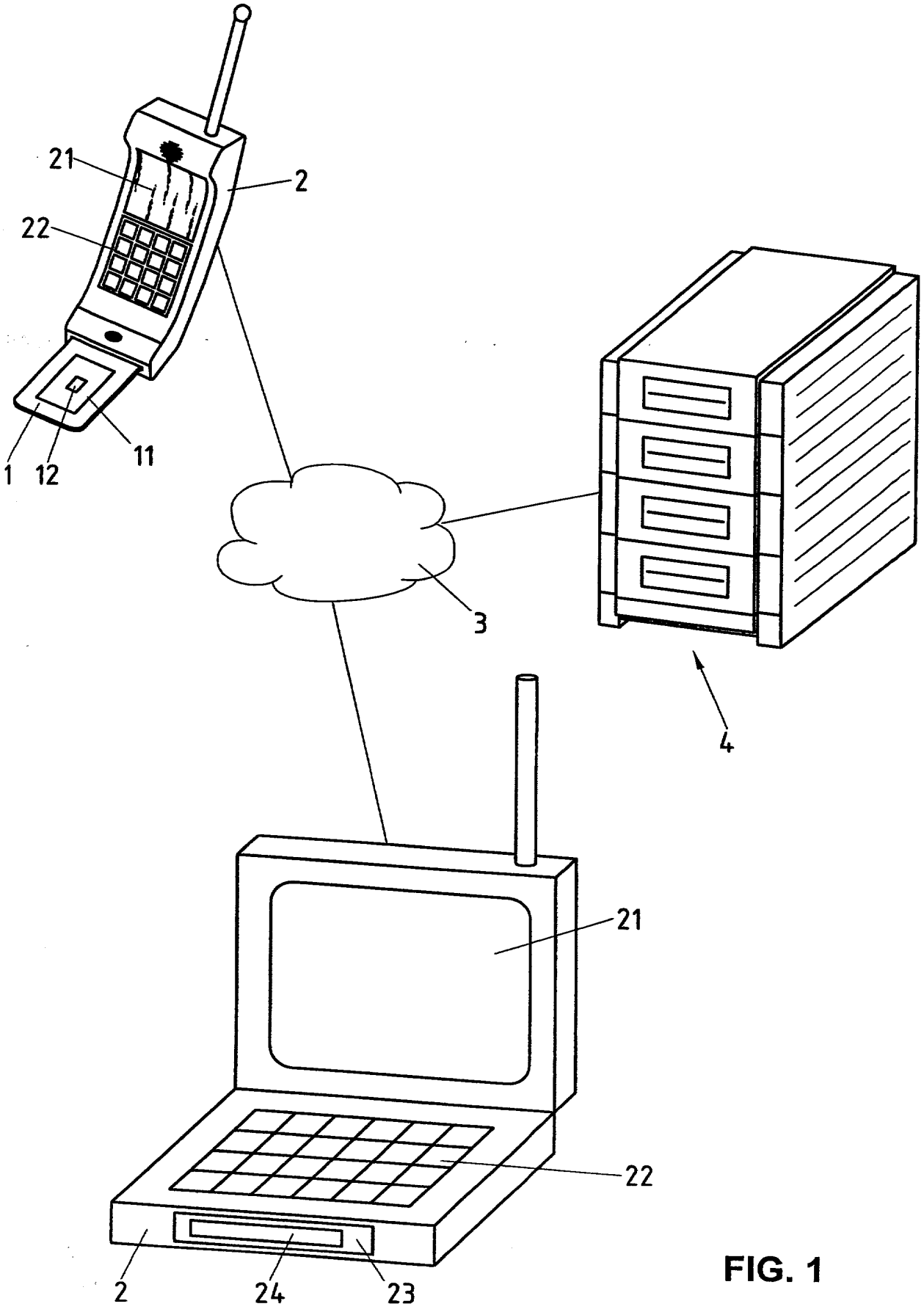

FIG. 1

Declaration and Power of Attorney For Patent Application
Erklärung Für Patentanmeldungen Mit Vollmacht
German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

☐ _____

_____

_____,

deren Beschreibung

(zutreffendes ankreuzen)

☐ hier beigefügt ist.

☐ am _____ unter der

☐ Anmeldungsseriennummer _____

eingereicht wurde und am _____.
abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Method and Suitable Devices for Setting

the Degree of Security of Cryptography

Functions ,

the specification of which

(check one)

☒ is attached hereto.

☒ was filed on 21 July 1999 as

Application Serial No. PCT/CH 99/00336

and was amended on _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PTO/SB/103 (10-96)
Approved for use through 9/30/98. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

German Language Declaration

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäß Title 35, US-Code, § 119 (a)-(d), bzw. § 365(b) aller unten aufgeführten Auslandsanmeldungen für Patente oder Erfinderurkunden, oder § 365(a) aller PCT internationalen Anmeldungen, welche wenigstens ein Land ausser den Vereinigten Staaten von Amerika benennen, und habe nachstehend durch ankreuzen sämtliche Auslands-anmeldungen für Patente bzw. Erfinderurkunden oder PCT internationale Anmeldungen angegeben, deren Anmeldetag dem der Anmeldung, für welche Priorität beansprucht wird, vorangeht.

I hereby claim foreign priority under Title 35, United States Code, § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Applications
(Frühere ausländische Anmeldungen)

Priority Not Claimed
Priorität nicht beansprucht

(Number) (Nummer)	(Country) (Land)	(Day/Month/Year Filed) (Tag/Monat/Jahr der Anmeldung)	☐
---	---	---	
			☐

Ich beanspruche hiermit Prioritätsvorteile unter Title 35, US-Code, §119(e) aller US-Hilfsanmeldungen wie unten aufgezählt.

I hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s)listed below.

(Application No.) (Aktenzeichen)	(Filing Date) (Anmeldetag)

Ich beanspruche hiermit die mir unter Title 35, US-Code, § 120 zustehenden Vorteile aller unten aufgeführten US-Patentanmeldungen bzw. § 365(c) aller PCT internationalen Anmeldungen, welche die Vereinigten Staaten von Amerika benennen, und erkenne, insofern der Gegenstand eines jeden früheren Anspruchs dieser Patentanmeldung nicht in einer US-Patentanmeldung, bzw. PCT internationalen Anmeldung in in einer gemäß dem ersten Absatz von Title 35, US-Code, § 112 vorgeschriebenen Art und Weise offenbart wurde, meine Pflicht zur Offenbarung jeglicher Informationen an, die zur Prüfung der Patentfähigkeit in Einklang mit Title 37, Code of Federal Regulations, § 1.56 von Belang sind und die im Zeitraum zwischen dem Anmeldetag der früheren Patentanmeldung und dem nationalen oder im Rahmen des Vertrags über die Zusammenarbeit auf dem Gebiet des Patentwesen (PCT) gültigen internationalen Anmeldetags bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

(Application No.) (Aktenzeichen)	(Filing Date) (Anmeldetag)	(Status) (patented, pending, abandoned) (Status) (patentiert, schwebend, aufgegeben)

Ich erkläre hiermit, daß alle in der vorliegenden Erklärung von mir gemachten Angaben nach bestem Wissen und Gewissen der Wahrheit entsprechen, und ferner daß ich diese eidesstattliche Erklärung in Kenntnis dessen ablege, daß wissentlich und vorsätzlich falsche Angaben oder dergleichen gemäß § 1001, Title 18 des US-Code strafbar sind und mit Geldstrafe und/oder Gefängnis bestraft werden können und daß derartige wissentlich und vorsätzlich falsche Angaben die Rechtswirksamkeit der vorliegenden Patentanmeldung oder eines aufgrund deren erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend bennanten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent-und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Norman F. Oblon, Registration Number 24,618; Marvin J. Spivak, Registration Number 24,913; C. Irvin McClelland, Registration Number 21,124; Gregory J. Maier, Registration Number 25,599; Arthur I. Neustadt, Registration Number 24,854; Richard D. Kelly, Registration Number 27,757; James D. Hamilton, Registration Number 28,421; Eckhard H. Kuesters, Registration Number 28,870; Robert T. Pous, Registration Number 29,099; Charles L. Gholz, Registration Number 26,395; Vincent J. Sunderdick, Registration Number 29,004; William E. Beaumont, Registration Number 30,996; Steven B. Kelber, Registration Number 30,073; Robert F. Gnuse, Registration Number 27,295; Jean-Paul Lavalleye, Registration Number 31,451; Stephen G. Baxter, Registration Number 32,884; Martin M. Zoltick, Registration Number 35,745; Robert W. Hahl, Registration Number 33,893; Richard L. Treanor, Registration Number 36,379; Steven P. Weihrouch, Registration Number 32,829; John T. Goolkasian, Registration Number 26,142; Marc R. Labgold, Registration Number 34,651; William J. Healey, Registration Number 36,160; Richard L. Chinn, Registration Number 34,305; Steven E. Lipman, Registration Number 30,011; Carl E. Schlier, Registration Number 34,426; James J. Kulbaski, Registration Number 34,648; Catherine B. Richardson, Registration Number 39,007; Richard A. Neifeld, Registration Number 35,299; and J. Derek Mason, Registration Number 35,270; with full powers of substitution and revocation.

30

Telefongespräche bitte richten an: *(Name und Telefonnummer)*

Direct Telephone Calls to: *(name and telephone number)*

(703) 413-3000

Postanschrift:

Send Correspondence to:

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
FOURTH FLOOR
1755 JEFFERSON DAVIS HIGHWAY
ARLINGTON, VIRGINIA 22202 U.S A.

Voller Name des einzigen oder ursprünglichen Erfinders: Adriano HUBER	Full name of sole or first inventor
Unterschrift des Erfinders — Datum: 18.11.2001	Inventor's signature — Date
Wohnsitz: 6600 Locaron (Switzerland) CH	Residence
Staatsangehörigkeit: Switzerland	Citizenship
Postanschrift: Via F. Caponelli 35 6600 Locarno (Switzerland)	Post Office Address
Voller Name des zweiten Miterfinders (falls zutreffend)	Full name of second joint inventor, if any
Unterschrift des Erfinders — Datum	Second Inventor's signature — Date
Wohnsitz	Residence
Staatsangehörigkeit	Citizenship
Postanschrift	Post Office Address

(Bitte entsprechende informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors.)